EXHIBIT 33

Назад к списку

Скрытые майнеры в Java-библиотеке и обвинения Google

freedmanclub.com • 13 Декабрь 2021 09:33, UTC

Время прочтения: ~2 м

Хакеры использовали сильнейшую уязвимость библиотеки логирования Apache Log4j на базе Java для того, чтобы установить скрытых майнеров и прочие опасные программы. О таком происшествии рассказали эксперты Netlab 360.

Эксплойт, называемый Log4Shell дал возможность преступникам внедрить опасные программы Mirai и Muhstik. В последствии они использовались для запуска криптомайнеров Kinsing, проведения крупнейших DDoS-атак, а также для внедрения маяков Cobalt Strike, которые занимались бы поиском наиболее уязвимых серверов.

Выявленные экспертами атаки были направлены на устройства под управлением Linux.

> «В настоящее время не были зафиксированы случаи эксплуатации уязвимости вымогательскими или APT-группировками, однако факт развертывания маяков Cobalt Strike указывает на предстоящее вредоносные кампании», – указали эксперты.

Эксперты компании Netlab 360 дали некое руководство пользователям — обновить сервер до версии Log4j.
Компания Cybereason в свою очередь разработала так называемую «вакцину». Она способна отключить параметр trustURLCodebase на Log4j, а значит она сделает уровень уязвимости ниже.

Важно, что в самом начале зимы экспертами Neodyme была обнаружена неполадка в библиотеке программ протокола Solana. Ошибка была достаточно опасна и давала возможность для кражи средств у DeFi-проектов со скоростью приблизительно $27 млн/час.

Обвинения Google

Во всем произошедшем Google обвинил двоих россиян.

Суд Нью-Йорка получил иск от корпорации Google против создателей ботнета Glupteba. Программа заразила приблизительно миллион компьютеров, которые базировались на Windows. Об этом происшествии сообщили эксперты TechCrunch.

Корпорация говорит о том, что виновниками данного происшествия вероятно являются два жителя России — Дмитрий Старовиков и Александр Филиппов, она ссылается данные, которые хранятся на их учетных записях Gmail и Google Workspace. В иске, так же, были упомянуты 15 лиц.

Эксперты внимательно наблюдали за действиями ботнета Glupteba еще с прошлого года. Программа ворует учетные записи пользователей Google, затем занимается майнингом и в конце настраивает прокси для перенаправления трафика.

Большая часть ПК было заражено путем загрузки бесплатных программ с различных сайтов. Количество пострадавших в разы увеличивается с каждым днем.

Данная система работает на блокчейне, дабы избежать сбоев, а также невозможно ее в полной мере обезвредить из-за «технической сложности». Когда на одном из серверов Glupteba отключается, то ботнет тут же сканирует распределенную сеть с целью найти новый адрес домена.

> «В любой момент мощности ботнета Glupteba могут быть применены в масштабной DDoS-атаке или для работы программ-вымогателей», – сказано в жалобе Google.

Корпорация предъявляет требование о возмещении ущерба, который нанесли разработчики, а также советуют навсегда прекратить использование всех сервисов Google.

Автор: Анастасия Запольская, аналитик Freedman Club Crypto News

Источник

← Назад к списку

Новости

Главные
Все новости
Видео
Биткоин
DeFi
NFT
Эфириум
Альткоины
Блокчейн
Майнинг
Финансы
Metaverse
Регулирование
Безопасность
Аналитика
Рынок
Прочее
GameFi
ICO

О нас

О проекте
Контакты
Политика конфиденциальности
Дисклеймер
Правообладателям

Статьи

Все статьи
Новости
Инвестиции
Регулирование
Технологии
Гест-посты
Аналитика
Новости партнеров
Начинающим

Реклама

Мероприятия

Глоссарий

Приложение

О приложении

Скачайте приложение **Crypto News** и получайте мировые новости криптовалюты и технологии блокчейн из разных источников:

Download on the App Store Get it on Google Play

Подписывайтесь на нас в социальных сетях:

Back to list

Hidden Miners in the Java Library and Google's Accusations

freedmanclub.com • 13 December 2021 09:33 UTC

Reading time: ~2 m

Hackers exploited a powerful vulnerability in the Java-based Apache Log4j logging library to install hidden miners and other dangerous programs. Netlab 360 experts told about such an incident.

An exploit called Log4Shell made it possible for criminals to inject dangerous Mirai and Muhstik programs. Subsequently, they were used to launch Kinsing cryptominers, carry out the largest DDoS attacks, as well as to introduce Cobalt Strike beacons that would search for the most vulnerable servers.

The attacks identified by experts were directed at devices running Linux.

> "Currently, there have been no cases of exploitation of the vulnerability by ransomware or APT groups,

> however, the deployment of Cobalt Strike beacons indicates an upcoming malicious campaign," the experts said.

Netlab 360 experts gave some guidance to users - upgrade the server to the Log4j version.

Cybereason, in turn, has developed a so-called "vaccine". It is able to disable the trustURLCodebase parameter on Log4j, which means it will make the vulnerability level lower.
It is important that at the very beginning of winter, Neodyme experts discovered a problem in the Solana protocol software library. The mistake was quite dangerous and made it possible to steal funds from DeFi projects at a rate of approximately $27 million/hour.

Google accusations

Google blamed two Russians for everything that happened.

A New York court has received a lawsuit from Google against the creators of the Glupteba botnet. The program infected approximately one million Windows-based computers. This incident was reported by TechCrunch experts.

The corporation says that the perpetrators of this incident are probably two residents of Russia - Dmitry Starovikov and Alexander Filippov, she refers to the data that is stored on their Gmail and Google Workspace accounts. The lawsuit also mentioned 15 persons.

Experts have been closely watching the actions of the Glupteba botnet since last year. The program steals Google user accounts, then mines, and finally sets up a proxy to redirect traffic.

Most PCs have been infected by downloading free programs from various websites. The number of victims is increasing exponentially every day.

This system works on the blockchain in order to avoid failures, and it is also impossible to completely neutralize it due to "technical complexity". When Glupteba goes down on one of the servers, the botnet immediately scans the distributed network in order to find a new domain address.

> "At any moment, the power of the Glupteba botnet can be used in a large-scale DDoS attack or ransomware," Google said in a complaint.

The corporation claims damages caused by the developers, and also advises to permanently stop using all Google services.

Author: Anastasia Zapolskaya, analyst at Freedman Club Crypto News

A source

← Back to list

news

Main
All news
Video
bitcoin
DeFi
NFTs
Ethereum

Altcoins
Blockchain
Mining
Finance
Metaverse
Regulation
Security

Analytics
Market
Other
game fi
ICO

About Us

about the project
Contacts
Privacy Policy
Disclaimer
Copyright holders

Articles

All articles
news
Investments
Regulation
Technology
Guest posts
Analytics
Partner news
Beginners

Advertising

Events

Glossary

Appendix

About the application